UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/925,503	08/10/2001	Victor I. Sheymov	741946-30	7363

22204 7590 07/05/2007

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	**PAPER NUMBER**
2137	
MAIL DATE	**DELIVERY MODE**
07/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/925,503	SHEYMOV ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *31,33-35,38-61,63-65 and 68-91* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *31,33-35,38-61,63-65 and 68-91* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Remarks

Claims 31, 33-35, 38-61, 63-65, and 68-91 are pending.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/13/2007 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 31, 33-35, 38, 39, 41-54, 56-61, 63-65, 68, 69, 71-84, and 86-91 are rejected under 35 U.S.C. 103(a) as being unpatentable over Comay (U.S. Patent 6,363,489) in view of Pearson (U.S. Patent 6,990,591) and Boebert (U.S. Patent 5,864,683).

Regarding Claim 31,

Comay discloses a system for protecting a distributed network from unauthorized access, comprising:

An intrusion detection system (Column 4, line 61 to Column 5, line 14), including:

An intrusion detection module (Column 4, line 61 to Column 5, line 14);

A communications management module coupled to the intrusion detection module (Column 4, line 61 to Column 5, line 14);

Intrusion analysis system coupled to the intrusion detection system (Column 5, lines 15-60), and including:

An intrusion analysis module (Column 5, lines 15-43), and

An intrusion reaction coordination module coupled to the intrusion analysis module (Column 5, lines 15-43),

Wherein the intrusion detection module detects a possible unauthorized access attempt into or within a distributed network being protected (Column 4, line 61 to Column 5, line 14);

The communications management module is coupled to the intrusion analysis module and forwards to the intrusion analysis module information regarding the detected possible unauthorized access attempt (Column 5, lines 15-43);

The intrusion analysis module determines based on the information regarding the detected possible unauthorized access attempt whether or

not the detected possible access attempt is authorized (Column 5, lines 15-60);

If the intrusion analysis module determines that the detected possible unauthorized access attempt is authorized, the intrusion analysis module forwards, via the communications management module, information to the intrusion detection module that the possible unauthorized access attempt is authorized (Column 5, lines 15-31); and

If the intrusion analysis module determines that the detected possible unauthorized access attempt is not authorized, the intrusion analysis module determines, via the intrusion reaction coordination module, appropriate actions, including forwarding information regarding the detected unauthorized access attempt to a monitoring center, and processing information from the monitoring center regarding the detected unauthorized access attempt (Column 5, lines 32-60; and Column 6, lines 57-68);

Wherein the intrusion analysis system in cooperation with the intrusion detection system enable communications between the monitoring center and an entity attempting the unauthorized access attempt without the entity being made aware that the entity attempting the unauthorized access attempt is communicating with the monitoring center (Column 5, lines 32-60); and

The monitoring center sends information to the analysis system and intended for the entity attempting the unauthorized access attempt, the analysis system substitutes origin information of the monitoring center from the received information with origin information of a target of the unauthorized access attempt and forwards the substituted information to the entity attempting the unauthorized access attempt, whereby it appears to the entity attempting the unauthorized access attempt that communications are continuing with the target of the unauthorized access attempt (Column 5, lines 32-60);

But does not explicitly disclose that the monitoring center is external to the distributed network being protected; and engaging the entity attempting the unauthorized access attempt to determine the location or origin of the entity attempting the unauthorized access attempt.

Pearson, however, discloses that the monitoring center is external to the distributed network being protected (Column 6, line 33 to Column 7, line 29). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the remote monitoring center of Pearson into the intrusion detection system of Comay in order to provide remote management for the intrusion detection systems of multiple sites, such that small business can afford to obtain up-to-date intrusion detection and protection, while allowing specialized personnel to

remotely and dynamically update the protection as required by new intrusions.

Boebert, however, discloses engaging the entity attempting the unauthorized access attempt to determine the location or origin of the entity attempting the unauthorized access attempt (Column 15, lines 24-33; Column 16, lines 52-65; and Column 28, lines 15-28).. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the attack countermeasures of Boebert into the intrusion detection system of Comay as modified by Pearson in order to allow the system to trace the attacker, even when the attack is using spoofed addresses, thereby determining the true location of the attacker and/or to provide the attack with covert identification data that can be used to prove that the data was stolen from the network.

Regarding Claim 61,

Claim 60 is a method claim that corresponds to system claim 31 and is rejected for the same reasons.

Regarding Claim 91,

Claim 91 is a computer readable medium claim that corresponds to system claim 31 and is rejected for the same reasons.

Regarding Claim 33,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Pearson discloses that the intrusion analysis

system communicates with the monitoring center via a secure tunnel (Column 20, lines 38-50).

Regarding Claim 63,

Claim 63 is a method claim that corresponds to system claim 33 and is rejected for the same reasons.

Regarding Claim 34,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that the communications from the monitoring center to the entity attempting the unauthorized access attempt are modified, via the intrusion analysis system and the intrusion detection system, to appear as if the communications originate from the distributed network being protected (Column 5, lines 32-60).

Regarding Claim 64,

Claim 64 is a method claim that corresponds to system claim 34 and is rejected for the same reasons.

Regarding Claim 35,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that the intrusion analysis system logs information regarding communications with the entity attempting the unauthorized access attempt (Column 5, lines 15-31).

Regarding Claim 65,

Claim 65 is a method claim that corresponds to system claim 35 and is rejected for the same reasons.

Regarding Claim 38,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses detecting that the possible unauthorized access attempt into the distributed network being protected is external to the network being protected (Column 4, line 61 to Column 5, line 31), and Boebert discloses detecting that the possible unauthorized access attempt is internal to the network being protected (Column 7, lines 43-54; Column 12, lines 43-58; Column 29, lines 47-58; and Column 30, lines 59-67).

Regarding Claim 68,

Claim 68 is a method claim that corresponds to system claim 38 and is rejected for the same reasons.

Regarding Claim 39,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses the intrusion detection module forwards via the communications management module information regarding the possible unauthorized access attempt to the intrusion analysis module, and the intrusion analysis module evaluates the received information and if the intrusion analysis module determines that the possible unauthorized access attempt is not authorized, the intrusion

analysis module determines whether or not a retaliatory action should be taken, including handling the unauthorized access attempt internally or providing information to the monitoring center regarding the unauthorized access attempt (Column 5, lines 15-60), and Boebert discloses that the possible unauthorized access attempt is internal to the network being protected (Column 7, lines 43-54; Column 12, lines 43-58; Column 29, lines 47-58; and Column 30, lines 59-67).

Regarding Claim 69,

Claim 69 is a method claim that corresponds to system claim 39 and is rejected for the same reasons.

Regarding Claim 41,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses a database, wherein the intrusion analysis module employs the database, including information regarding previous unauthorized access attempts, to determine whether or not the detected possible unauthorized access attempt is authorized (Column 5, lines 15-31).

Regarding Claim 71,

Claim 71 is a method claim that corresponds to system claim 41 and is rejected for the same reasons.

Regarding Claim 42,

Comay as modified by Pearson and Boebert discloses the system of claim 41, in addition, Comay discloses that the database includes profiles of information related to one or more entities associated with the previous unauthorized access attempts, including origin information regarding the previous unauthorized access attempts (Column 5, lines 15-31).

Regarding Claim 72,

Claim 72 is a method claim that corresponds to system claim 42 and is rejected for the same reasons.

Regarding Claim 43,

Comay as modified by Pearson and Boebert discloses the system of claim 41, in addition, Comay discloses that the intrusion analysis module is configured to query the database to determine whether or not the possible unauthorized access attempt is an error in communications, including a bit error (Column 4, line 61 to Column 5, line 31).

Regarding Claim 73,

Claim 73 is a method claim that corresponds to system claim 43 and is rejected for the same reasons.

Regarding Claim 44,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that the intrusion analysis module is configured to determine based on historical profiles, and

previous unauthorized access attempts whether or not the detected possible unauthorized access attempt is authorized (Column 5, lines 15-31).

Regarding Claim 74,

Claim 74 is a method claim that corresponds to system claim 44 and is rejected for the same reasons.

Regarding Claim 45,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that the intrusion reaction coordination module determines the appropriate actions based on a number of previous unauthorized access attempts, and a nature of the unauthorized access attempt, including destructiveness of packets received during the unauthorized access attempt (Column 5, lines 15-60; and Column 6, lines 57-68).

Regarding Claim 75,

Claim 75 is a method claim that corresponds to system claim 45 and is rejected for the same reasons.

Regarding Claim 46,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that the intrusion reaction coordination module, to determine the appropriate actions, analyzes the information received by the intrusion detection module, historical

information regarding unauthorized access attempts, source and destination ports of unauthorized access attempts, and IP address information of unauthorized access attempts (Column 5, lines 15-60); and

Pearson discloses receiving information from a central repository that catalogs information related to unauthorized access attempts from one or more other protected networks (Column 7, lines 30-39).

Regarding Claim 76,

Claim 76 is a method claim that corresponds to system claim 46 and is rejected for the same reasons.

Regarding Claim 47,

Comay as modified by Pearson and Boebert discloses the system of claim 46, in addition, Pearson discloses that the analysis is based on at least one of a look-up table, a neural network analysis, and a predetermined event sequence (Column 8, lines 10-32).

Regarding Claim 77,

Claim 77 is a method claim that corresponds to system claim 47 and is rejected for the same reasons.

Regarding Claim 48,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that if the intrusion reaction coordination module determines that a responsive or retaliatory action is not required, the intrusion reaction coordination module instructs the

intrusion detection module to block communications from an entity attempting the unauthorized access attempt (Column 5, lines 15-60; and Column 6, lines 57-68).

Regarding Claim 78,

Claim 78 is a method claim that corresponds to system claim 48 and is rejected for the same reasons.

Regarding Claim 49,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that if the intrusion reaction coordination module determines that a responsive or retaliatory action is not required, the intrusion reaction coordination module instructs the intrusion detection module to block communications from an entity that matches one or more characteristics of the unauthorized access attempt (Column 5, lines 15-60; and Column 6, lines 57-68).

Regarding Claim 79,

Claim 79 is a method claim that corresponds to system claim 49 and is rejected for the same reasons.

Regarding Claim 50,

Comay as modified by Pearson and Boebert discloses the system of claim 41, in addition, Comay discloses that the intrusion reaction coordination module logs information regarding an entity attempting the

unauthorized access attempt to the database for use in a future unauthorized access attempt by the entity (Column 5, lines 15-31).

Regarding Claim 80,

Claim 80 is a method claim that corresponds to system claim 50 and is rejected for the same reasons.

Regarding Claim 51,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that the intrusion analysis module is configured to store information regarding an address to which the unauthorized access attempt was directed for use by the intrusion reaction coordination module to determine the appropriate actions (Column 5, lines 15-31).

Regarding Claim 81,

Claim 81 is a method claim that corresponds to system claim 51 and is rejected for the same reasons.

Regarding Claim 52,

Comay as modified by Pearson and Boebert discloses the system of claim 41, in addition, Comay discloses that upon receipt of a communication from the monitoring center, the intrusion detection system in cooperation with the intrusion analysis system analyze the communication, determines address information of a source of the communication from the monitoring center, and removes the address

information from the communication from the monitoring center leaving the remaining information for further analysis (Column 4, line 61 to Column 5, line 60).

Regarding Claim 82,

Claim 82 is a method claim that corresponds to system claim 52 and is rejected for the same reasons.

Regarding Claim 53,

Comay as modified by Pearson and Boebert discloses the system of claim 52, in addition, Comay discloses that the address information of the source of the communication from the monitoring center is stored in the database, and the intrusion analysis module is configured to use the address information to communicate information to the monitoring center (Column 5, lines 15-60), including information regarding a response to a password request by an entity attempting the unauthorized access attempt (Column 8, lines 9-26).

Regarding Claim 83,

Claim 83 is a method claim that corresponds to system claim 53 and is rejected for the same reasons.

Regarding Claim 54,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that the intrusion detection system in cooperation with the intrusion analysis system conceals the

identity of the monitoring center, communicates information with the monitoring center, and screens underlying content in the communicated information, including removing sensitive information from the communicated information (Column 5, lines 32-60).

Regarding Claim 84,

Claim 84 is a method claim that corresponds to system claim 54 and is rejected for the same reasons.

Regarding Claim 56,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that the intrusion detection system and the intrusion analysis system cooperate with the monitoring center to aid in detecting a source of the unauthorized access attempt (Column 4, line 61 to Column 5, line 60).

Regarding Claim 86,

Claim 86 is a method claim that corresponds to system claim 56 and is rejected for the same reasons.

Regarding Claim 57,

Comay as modified by Pearson and Boebert discloses the system of claim 56, in addition, Comay discloses that the intrusion detection system in cooperation with the intrusion analysis system receives from the monitoring center information regarding unauthorized accesses or access attempts into distributed networks (Column 5, lines 32-60).

Regarding Claim 87,

Claim 87 is a method claim that corresponds to system claim 57 and is rejected for the same reasons.

Regarding Claim 58,

Comay as modified by Pearson and Boebert discloses the system of claim 57, in addition, Comay discloses that the intrusion detection system in cooperation with the intrusion analysis system analyzes the information regarding unauthorized accesses or access attempts into the distributed networks received from the monitoring center to determine if the received information matches a profile or has characteristics to one or more known unauthorized access attempts (Column 5, lines 32-60).

Regarding Claim 88,

Claim 88 is a method claim that corresponds to system claim 58 and is rejected for the same reasons.

Regarding Claim 59,

Comay as modified by Pearson and Boebert discloses the system of claim 58, in addition, Comay discloses that upon detection of an unauthorized access attempt, the intrusion detection system in cooperation with the intrusion analysis system forwards information regarding the unauthorized access attempt to the monitoring center (Column 5, lines 32-60); and

Pearson discloses including information regarding unauthorized access attempts in a central database that maintains information regarding the unauthorized accesses or access attempts into the distributed networks (Column 20, lines 38-50).

Regarding Claim 89,

Claim 89 is a method claim that corresponds to system claim 59 and is rejected for the same reasons.

Regarding Claim 60,

Comay as modified by Pearson and Boebert discloses the system of claim 31, in addition, Comay discloses that the system is implemented with one or more hardware and or software components (Column 4, lines 48-60).

Regarding Claim 90,

Claim 90 is a method claim that corresponds to system claim 60 and is rejected for the same reasons.

3. Claims 40, 55, 70, and 85 are rejected under 35 U.S.C. 103(a) as being unpatentable over Comay in view of Pearson and Boebert, further in view of Lyle (U.S. Patent 6,886,102).

Regarding Claim 40,

Comay as modified by Pearson and Boebert discloses the system of claim 31, but does not disclose that the monitoring center includes a law enforcement entity.

Lyle, however, discloses that the monitoring center includes a law enforcement entity (Column 1, lines 39-54). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the DoS protection system of Lyle into the intrusion detection system of Comay as modified by Pearson and Boebert in order to provide a mechanism by which to share attack information dynamically and automatically between networks, allowing networks to cooperate on tracing an attack and to take corrective actions regarding the attack (Column 2, lines 20-31).

Regarding Claim 70,

Claim 70 is a method claim that corresponds to system claim 40 and is rejected for the same reasons.

Regarding Claim 55,

Comay as modified by Pearson and Boebert discloses the system of claim 54, in addition, Comay discloses that the intrusion detection system in cooperation with the intrusion analysis system screens and removes sensitive information, such as removing content originating from a predetermined location (Column 5, lines 32-60), but does not disclose using a policy file to regulate the screening and removing of the sensitive

information, including removing all content or core information, removing content having certain words, and removing content originating from a predetermined location.

Lyle, however, discloses using a policy file to regulate the screening and removing of the sensitive information, including removing all content or core information, and removing content having certain words (Column 9, line 66 to Column 10, line 43). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the DoS protection system of Lyle into the intrusion detection system of Comay as modified by Pearson and Boebert in order to provide a mechanism by which to share attack information dynamically and automatically between networks, allowing networks to cooperate on tracing an attack and to take corrective actions regarding the attack (Column 2, lines 20-31).

Regarding Claim 85,

Claim 85 is a method claim that corresponds to system claim 55 and is rejected for the same reasons.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER